**In the Claims**

1. (previously presented) A method of re-authenticating and protecting wireless communication security comprising the steps of:

a) performing a secondary authentication protocol between a wireless client electronic system (client) and a wireless network access point electronic system (AP) using a key lease generated by performance of a primary authentication protocol, wherein said key lease includes a key lease period for indicating a length of time in which said key lease is valid for using said secondary authentication protocol instead of said primary authentication protocol, and wherein the secondary authentication protocol includes the steps of:

a(i) transmitting said key lease from said client to said AP;

a(ii) generating a first random number associated with said client and a second random number associated with said AP, wherein said key lease includes an encryption key for use in said secondary authentication protocol; and

a(iii) transmitting said first random number to said AP and said second random number to said client; and

b) if said secondary authentication protocol is successful, generating a session encryption key for encrypting communication traffic between said client and said AP, wherein the generating comprises:

b(i) applying a hash function and said encryption key to said first random number and said second random number to determine said session encryption key.

2. (cancelled)

3. (cancelled)

4. (previously presented) A method as recited in claim 1 wherein said hash function is a HMAC-MD5 algorithm and wherein said hash function and encryption key are applied to a concatenation of said first random number and said second random number to determine said session encryption key.

5. (previously presented) A method as recited in claim 1 wherein said hash function is a HMAC-SHA-1 algorithm and wherein said hash function and encryption key are applied to a concatenation of said first random number and said second random number to determine said session encryption key.

6. (previously presented) A method as recited in claim 1 wherein said step b) includes:

generating a first session encryption key for encrypting communication traffic from said client to said AP; and

generating a second session encryption key for encrypting communication traffic from said AP to said client.

7. (previously presented) A method as recited in Claim 6 wherein said step b) includes:

using said encryption key, said first random number, said second random number, a first media access control (MAC) address associated with said client, a second media access control (MAC) address associated with said AP, and the hash function to determine said first and second session encryption keys.

8. (previously presented) A method as recited in Claim 7 wherein said hash function is a HMAC-MDS algorithm and wherein said hash function and said encryption key are applied to a concatenation of said first random number, said second random number, said first media access control (MAC) address associated with said client, and said second media access control (MAC) address associated with said AP to determine said first session encryption key.

9. (previously presented) A method as recited in Claim 7 wherein said hash function is a HMAC-SHA-1 algorithm and wherein said hash function and said encryption key are applied to a concatenation of said first random number, said second random number, said first media access control (MAC) address associated with said client, and said second media access control (MAC) address associated with said AP to determine said first session encryption key.

10. (previously presented) A method as recited in Claim 7 wherein said said hash function is a HMAC-MD5 algorithm and said hash function and said encryption key are applied to a concatenation of said first random number, said second random number, said second media access control (MAC) address associated with said AP, and said first media access control (MAC) address associated with said client to determine said second session encryption key.

11. (currently amended) A method as recited in Claim 7 wherein said hash function is a HMAC-SHA-1 algorithm and said hash function and said encryption key are applied to a concatenation of said first random number, said second random number, said second media access control (MAC) address associated with said AP, and said first media access control (MAC) address associated with said client to determine said second session encryption key.

12. - 72. (cancelled)